ProPartner Network

From Risk to Revenue: 6 Resilience Trends and 4 Tools for Partners

Safely unlock the value of AI and digital innovation

Ransomware and disruptive incidents aren't slowing down. Data trust and resilience depends on clear ownership, tested recovery, and the right controls. Partners can turn risk into revenue with the following trends and tips from the Data Trust and Resilience Report 2026.

01 Close the "confidence gap"

- **90%** of leaders are confident they'll hit recovery time objectives (RTOs), but among orgs with incidents, **40%+** still reported disruption or financial loss.

Customers *think* they're covered, but partners can **lead assessment and validation** services to prove (or disprove) real recoverability.

02 Ransomware recovery outcomes are the wake-up call

- Only **28%** fully recovered all affected data after ransomware-related operational loss/encryption.

Position clean **recovery, immutability, and recovery testing** as non-negotiable.

03 AI is turning resilience into a data governance and visibility problem

- **43%** say AI adoption is outpacing their ability to secure data/models.
- **42%** have limited visibility into AI tools/models in use.
- **40%** haven't updated policies for AI-specific risks; **25%** cite shadow/unauthorized AI tools as a primary concern.

Package **AI data governance readiness** (e.g., visibility, acceptable-use, control enforcement) as a new consulting offer that's tied to resilience.

04 Policy doesn't reduce risk, enforced controls do

- **48%** have Data Loss Prevention (DLP) in place; orgs with DLP report better visibility and less "AI outpacing security."

Partners can add value with Implementation and operationalization projects (e.g., controls, monitoring, workflows).

05 Proven recovery with testing as the proof point

- Resilience is framed as **tested and validated recovery**, not assumed capability.
- Measure what matters: Common KPIs tracked: Recovery testing (**57%**), mean time to recover (**56%**), time to isolate/contain (**42%**), and automated/orchestrated recovery (**23%**).

Lead with **disaster recovery** (DR) **tabletop and technical recovery tests**, then move to managed recurring testing and reporting.

06 Executive alignment and cross-functional ownership correlates with better outcomes

- AI/data risk governance is usually owned by a single executive, and only **17%** reported cross-functional governance structure.

Offer governance operating models (e.g., RACI, steering committee cadence, board-ready reporting) as an accelerator to deployment success.

Make it actionable

Four key deliverables to add to your toolbox:

- **A resilience assessment** that outlines visibility, alignment of RTOs to business continuity, and gap analysis.
- **Recovery validation services** that perform restore tests, ransomware scenario tests, and clean-room recovery patterns.
- **AI data governance readiness** that covers AI tool discovery, policy-to-control implementation, and shadow AI containment.
- **An executive reporting pack**, including KPIs, that are insurer and compliance-aligned delivered in a regular (i.e. monthly) cadence.

→ Read the full report here